REMARKS

Applicant respectfully requests reconsideration. Claims 2, 4, 9-13, 15-20 and 43-65 were previously pending in this application. By this amendment, claims 10, 15, 16, 51, 58 and 59 have been amended. As a result, claims 2, 4, 9-13, 15-20 and 43-65 are pending for examination. No new matter has been added.

Allowable Subject Matter

Claims 9, 15-16, 20, 49-50, 52-53 and 60-65 were indicated to contain allowable subject matter.

Claim 51 has been amended to incorporate limitations of dependent claims 15 and 16, which were indicated to be allowable. Accordingly, Applicants believe that independent claim 51 as amended should be allowed. Based on these amendments, dependent claims 17-19 and 54-56 should also be allowed.

Further, Applicants respectfully submit that dependent claim 11 should also be included in the list of claims reciting allowable subject matter because it depends from claim 49, which is indicated to be allowable.

Rejections Under 35 U.S.C. §102

Each of the independent claims 43, 57, 58 and 59 has been rejected under 35 U.S.C. §102 based on Nyman (2003/0037033). Applicants respectfully disagree that Nyman teaches all limitations of any of the independent claims.

Prior to discussing the claims individually, Applicants provide a brief summary of some embodiments disclosed in the present specification and the Nyman reference. This summary is not intended to characterize the claims or any of the terms used in the claims.

Briefly, the specification describes a peer-to-peer collaboration system in which each user may respond to events, such as messages from other users. The response may be based on an authentication level of the user initiating the event. The application describes at least three levels of authentication, including certified, authenticated or unauthenticated. A user may be certified, for example, by a network administrator. In contrast, a user may be authenticated for purposes

of processing an event by a computing device based on input from a user of that computing device. Users that are not certified or authenticated may be regarded as unauthenticated.

The present application describes that even these unauthenticated users may be authenticated through a process of "implicit authentication" [14, 60]. Implicit authentication is implemented on a computing device by storing contact information for other users with which the user of the computing device has communicated. Subsequent communications from the same users may be treated as authenticated. This implicit authentication may be used in combination with warnings to the user of the computing device to block others from masquerading as authenticated users.

Specifically, in the peer-to-peer collaboration system, users have both an identity and a display name. While the identity may be unique, display names may be the same or very similar. As a result, a user may communicate unintentionally with an unauthenticated user, believing the unauthenticated user is in fact an intended authenticated user because they have the same or similar display names, which, may create security problems.

Levels of authentication of users may also be used to reduce the likelihood of security problems in a peer-to-peer collaboration system. Warnings or restrictions on communication may be imposed based on authentication levels such that a device selectively responds to events in accordance with a security policy.

The Nyman reference cited in the Final Office Action does not describe such a system. Rather, Nyman describes "name distribution messages" (see Abstract). The name distribution messages are generated by users about themselves. When transmitted to devices of other users, the name distribution messages may be used for automatically resolving name conflicts [0022], i.e., without further user interaction.

In rejecting all of the independent claims, the Office Action cites to Figures 1 and 2B and paragraphs 0036-0039 and 0091-0105 of Nyman. However, these portions of Nyman do not relate to either implicit authentication, warning of users or selectively responding to events in accordance with a security policy as in the present application.

To the contrary, FIG. 1, as described at paragraphs 0036-0039, pictures a user giving himself or herself a display name that is then communicated to other user devices when he or she

joins an ad hoc network. Specifically, FIG. 1 pictures "Alice's Device" 100 through which Alice can specify for herself a primary display name and an alternative display name that other devices will display in the event that the primary display name is already in use within the network.

The cited passage then describes that each device to join the ad hoc network communicates its primary display name and alternative display name through an ADD DEVICE message. FIG. 1A and paragraphs 0037-0039 describe that such messages are propagated from device to device in the ad hoc network, with the end result that devices in the ad hoc network can display the display names that other users have chosen for themselves. This process is described in connection with element 325 of FIG. 3E, and occurs automatically, without notice to or action by the user of the devices on which those names are displayed (¶0022).

FIG. 2B and the cited passages from 0091-0105 likewise do not describe warning a user or selectively responding to events as described in the present application. Rather, FIG. 2B depicts an internal data structure in Alice's device and indicates how names of other devices will be displayed. Though that data table includes a "conflict flag," there is no indication that the conflict flag is displayed to Alice, the user of the device. Moreover, there is no indication that the user Alice is even aware that such a conflict flag has been stored in her device, as Nyman expressly teaches that conflicts are resolved automatically (¶0022).

The cited passage at 0091-0105 also does not teach a system as described in the present application. To the contrary, that passage describes how a device joins an ad hoc network and whether, once it joins the network, it will be displayed on other user devices. Specifically:

- Paragraph 0091 describes the name manager table pictured in FIG. 2B, indicating that when a conflict exists, the alternative display name for device is used for one of the conflicting devices.
- Paragraphs 92-94 describe that a user (in the example provided, the user Mark) can indicate whether all other devices should display his name at all. If no blanket authorization is provided, then Mark must separately send authorization for his name to be displayed.
- Paragraph 95 describes the concept of "hop count" that is used in Nyman to ensure that only short range devices are displayed.

- Paragraphs 96-98 describe a time stamp used as part of resolution process 325 to automatically determine which device should use its alternative display name in the event a conflict is detected.
- Paragraphs 99-100 describe a "stop list" that may be specified by a user to block specific users or classes of devices from joining an ad hoc network.
- Paragraph 101 describes a mechanism by which a device that does not support the add device protocol of Nyman may join an ad hoc network.
- Paragraph 102 describes a display on a device in which only short range devices that have joined the network are displayed, each with a unique name.
- Paragraphs 103-104 describe that devices that receive an "ADD DEVICE" message propagate that message to other devices in the network.
- Paragraph 105 describes that more than one alternative device name could be provided in a name distribution message.

There is no indication in the cited passages or figures that a warning is generated on a display when there are equivalent names. Likewise, there is no indication in the cited passages or figures of any security policy options for selectively responding to an event, such as those described in the application that allow or restrict processing or allow processing with a warning. Thus, there are multiply differences between the system described in the present application and the system of the Nyman reference. At least one of these differences is reflected in each of the independent claims.

For example, independent claim 43 relates to a method of operating a computing device. The claim recites "generating a warning on a display associated with the computing device." The Office Action does not specifically identify any action of Nyman that constitutes a warning. To the contrary, as pointed out above, Nyman emphasizes automatic resolution of naming conflicts. Thus, Nyman does not meet this limitation of claim 43 and the rejection should be withdrawn.

As to independent claim 57, the claim recites "generating a warning on a display associated with the computing device." For reasons that should be apparent from the discussion

of the Nyman reference, above, the reference does not teach generating a warning as would be required to meet all limitations of claim 57. Thus, the rejection should be withdrawn.

Independent claim 58 also recites limitations not shown or suggested in Nyman. For example, claim 58 recites "selectively responding to the event based on the authentication level and a security policy, the security policy having at least an allow option, a restrict option and a warn option." There are multiple reasons why Nyman does not meet this limitation. Nyman does not describe a security policy. It follows that Nyman does not describe a security policy having at least three options, and certainly does not describe the allow, restrict and warn options that are recited in claim 58. Moreover, claim 58 continues with a recitation of actions performed when the security policy is determined to specify each of the three options. The Office Action identifies no selective response to any event that meets all limitations of claim 58. Thus, the rejection of claim 58 should be withdrawn.

Independent claim 59 also recites: "selectively responding to the event based on the authentication level and the security policy, the security policy having at least an allow option, a restrict option and a warn option." For reasons that should be apparent from the discussion of Nyman above, the reference does not describe a security policy. It follows that the reference does not describe a security policy having at least three options, as recited in claim 59. Moreover, the reference does not teach an allow option, a restrict option and a warn option, all of which would be required to meet the limitations of claim 59. Moreover, claim 59 recites the nature of the selective response when the security policy option is set to restrict and the authentication level is less than or equal to a threshold level. Because Nyman does not teach selectively responding at all, it follows that the reference does not teach the more detailed recitation of the nature of the response that would be required to meet all limitations of claim 59. For this additional reason, the rejection of claim 59 should also be withdrawn.

General Comments on Dependent Claims

Because each of the dependent claims depends from a base claim that is believed to be in condition for allowance, Applicants believe that it is unnecessary at this time to argue the allowability of each of the dependent claims individually. Applicants do not, however,

necessarily concur with the interpretation of the dependent claims as set forth in the Office Action, nor do Applicants concur that the basis for the rejection of any of the dependent claims is proper. Therefore, Applicants reserve the right to specifically address the patentability of the dependent claims in the future, if deemed necessary.

However, Applicants do point out that the dependent claims recite limitations that further distinguish the Nyman reference. For example, claim 4 recites further limitation on the act of generating a warning on a display associated with the computing device. Claim 10 similarly recites additional limitations on the act of generating the warning, specifically reciting "a dialog box having all displaying names that are equivalent."

As another example, claims 12 and 13 recite aspects of displaying the warning, which can not be met by Nyman because it does not describe displaying a warning at all. Claim 46 similarly recites further limitations on the manner of generating the warning that are not met by Nyman.

CONCLUSION

A Notice of Allowance is respectfully requested. The Examiner is requested to call the undersigned at the telephone number listed below if this communication does not place the case in condition for allowance.

If this response is not considered timely filed and if a request for an extension of time is otherwise absent, Applicant hereby requests any necessary extension of time. If there is a fee occasioned by this response, including an extension fee, the Director is hereby authorized to charge any deficiency or credit any overpayment in the fees filed, asserted to be filed or which should have been filed herewith to our Deposit Account No. 23/2825, under Docket No. M1103.70263US00.

Dated: 3/25/09

Respectfully submitted,

By

Edmund J. Walsh
Registration No.: 32,950
WOLF, GREENFIELD & SACKS, P.C.
Federal Reserve Plaza
600 Atlantic Avenue
Boston, Massachusetts 02210-2206
617.646.8000